Towards Interoperabilty in Identity Federation Systems

Elena M. Torroglosa-Garcia* and Antonio F. Skarmeta-Gomez
Department of Communication and Information Engineering
University of Murcia, 30100 Murcia, Spain
{emtg, skarmeta}@um.es

Abstract

Digital services aimed at humans need to ensure user identity. Governments and institutions confront the identity problem when migrating their face to face services to the digital world, where no facial identification is plausible. On the other hand, users concerns regarding their privacy and security are a barrier to be overcome during the migration. Identity federations are envisioned to unify and simplify user and service management through trust relationships. Recent trends indicate that federations are limited by target audiences and scope and are isolated from each other. It is necessary to go one step further and work in interoperability mechanisms to develop the existing federations and improve user experience and service quality. This work reviews some of the most important identity federations, with the focus on well defined sectors such as research and education communities and governments, specifically Moonshot, eduGAIN, EUDAT, STORK and EIDAS. Based on their analyses, we consider interfederation scenarios between eduGAIN, STORK and eIDAS and propose interoperability mechanisms to reach interfederation solutions to extend the user's scope of each o with the others and thus provide wider federation possibilities.

Keywords: Identity Federation, AAI, Interoperability, Authentiation, Digital Identity, SAML.

1 Introduction

The need to interconnect people and services is still growing. Companies are aware of the need to unite and offer common services as a way to win new users and simplify their management. Similarly, governments and institutions see the need to migrate their services to the digital world to cover the ever increasing demand for e-management, since it streamlines procedures and saves costs. In addition, users demand mechanisms that guarantee privacy and security in the use of IT systems while at the same time wanting every service to be connected and available. Public and private institutions and companies work hard to increase the use and quality of their networks and services and are always studying new ways to improve existing resources and to create new ones.

Identity federations allow arrangements between several companies that let subscribers get access to services and the network of all companies in the group using the same digital identity. These agreements enable services to be unified and user based management. In addition, Identity federations allow better privacy and security control of user personal data, so improving and simplifying the management and the interaction with service providers. Therefore, federation systems are especially interested in harmonizing and unifying users' interaction with public administration with the certainty that interoperability and authentication are critical for the successful advancement of digital technologies. In contrast, the increase in the number of federations, each focusing on different areas, revives the initial problem with the users need of having user accounts in each federation, and also implies the isolation of services and user due to the impossibility of interacting between them. Most existing interfederation solutions imply the

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 8:2 (June 2017), pp. 19-43

*Corresponding author: Department of Communication and Information Engineering, University of Murcia, Campus de Espinardo, 30100 Murcia, Spain, Tel: +34-868-884607 migration or adaptation of in-production services to new authentication and interoperation mechanisms. This can be a good option in the case of new deployments, but in the case of running federations and services, it might not be a practical if it entails the modification of entities and user flows, the migration to new protocols or the adoption of a complete new layer. All these changes usually imply the increase of operation complexity, number of rules and difficult political agreements.

We will review some of the most relevant identity federations in the education, government and research sectors as well as the general public in order to establish their main characteristics, with the focus on federations oriented to the administrative sector. Based on these, we raise the problems of interconnecting deployed federations. In order to solve them, we propose the introduction of a new intermediate entity, designed expressly for each case, which is in charge of acting as trust point between federations and translating between security protocols, digital identities and attributes.

The reminder of this paper is structured as follows: Section 2 an analysis of different Identity Federations such as Moonshot, eduGAIN, EUDAT, STORK and eIDAS. In Section 3 we describe several interoperability scenarios and propose interfederation solutions for each one. Finally, Section 4 offers an overview of this work.

2 Identity Federations: review

Any standard Internet user has to manage a large set of usernames and password throughout her day at Internet. Users consumes a wide variety of electronic services which oblige them to use different authentication credential in each one, in order to guarantee their identity privacy. Digital identity is formed in general by personal and working information, contacts, tastes and preferences. All these information can be requested by service providers as requisite to be able of providing or customizing the service offered. The reality is that any Internet user has to share part of her private information in order of using Internet services and users need the use specific tools to manage and control their credentials and shared information.

Identity Management systems offer users tools and mechanisms to help them in the task of control credentials and personal information. These mechanisms include from the credential management and privacy assurance to Single Sign-On among others. From the point of view of Service Providers, Identity Management systems allow the simplification of users management, thanks to delegate the authentication and credential storage.

Identity federations are based on the establishment of trust agreements between organizations that allow any user in the federation to access resources and services of any federated organization thanks to a unique digital identity, which is common to the whole federation. This federated identity, valid for all federated services, simplifies the credential control by the user and the user management by service providers.

Within identity federations, there are different types of entities that interact with end users. Service Providers are companies that offer any kind of Internet services from web services to network access. Identity Providers provides services related to identity and can be subdivided into different types depending on their specific role. The first subtype is the Authentication Provider, which is in charge of checking if an user is who claims to be and providing authentications statements to the Service Providers that request them. The second subtype is the Attribute Provider, which is responsible for storing and managing user information; they also provide attribute statements to the Service Providers's requests. Figure 1 shows an entity diagram with the entities described.

An usual configuration for these entities is one Identity Provider that provides authentication and attribute information to several Service Provider about a big amount of Users in each organization. In the case of identity federated systems, exists different possible topologies in function of how architectural

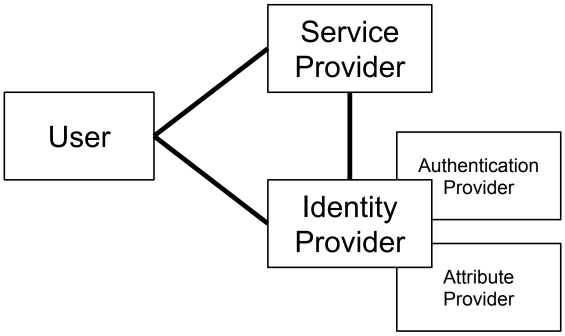

Figure 1: entities interaction diagram.

entities (Service Provides and Identity Providers) are configured. Some of the most usual topologies are: centralised, distributed and hierarchical. In centralised topologies, there is a central entity that concentrates interactions with other system participants. In distributed topologies, the load of work and responsibility is divided per interconnected groups or areas of work; some times this topology is similar to a mesh due to the high level of interconnections between entities. Finally, in hierarchical topologies the entities distribution are asymmetric with more elements in the ends, and less or even one when you move to the root. In this topology, the intermediate entities are able to attend the request with overload the root node. Figure 2 shows different examples of these configurations:

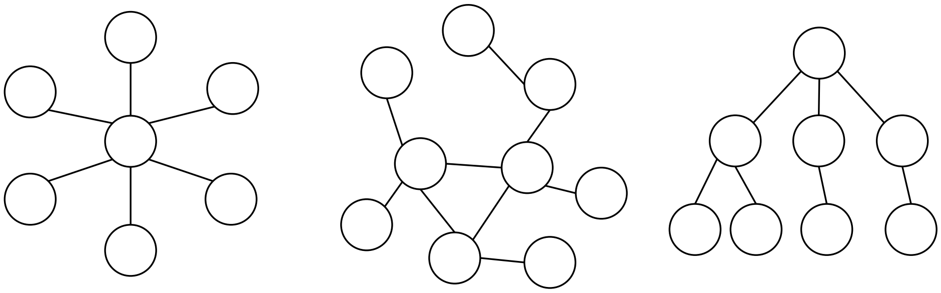

Figure 2: examples of possible topologies in identity federation systems. From left to right: centralised, distributed and hierarchical.

There are multiple identity federations that have been emerging to cover different needs and requirements. According to the kind of services offered, the target users, the area of deployment and the security requisites, we can move between a wide range of federations. Underneath, there are many technologies and protocols to interconnect and encode Authentication and Authorization Infrastructures (AAI), and some of the most common technologies are SAML 2.0, OpenID or OAuth2. Even when the underlying technology is the same between a federation and the new service, the federation process can be complex. The problems multiply exponentially when attempting the interconnection of two existing already deployed federations.

Due to the high number of federations, this paper focuses on identity federations based on SAML 2.0, since this is the authentication and authorization protocol par excellence. The Security Assertion Markup Language (SAML) [1] is a XML-based proposal by the OASIS consortium for the creation and exchange of security information. SAML defines both, the representation of the information and the protocols that are used to exchange this information. SAML assertions are the security statement format to transport information regarding a specific principal. To exchange them, SAML defines the use of several query/response protocols, like Authentication Request Protocol to request authentication information regarding a principal, and the Assertion Query and Request Protocol to obtain an assertion or Name Identifier Management Protocol to change the identifier given to a principal.

The following identity federation review analyses, by each federation, different aspects such as the general characteristics, its architecture and entities, the basic flow of interaction, relevant protocols and software as well as the target audience and the use scope.

2.1 Moonshot

Moonshot promotes the development of a single unifying technology for extending the benefits of federated identity to a broad range of non-Web services [2] all in a manner that gives these users Single Sign On (SSO). It was developed by Jisc, the UK's National Research and Education Network (NREN, also known as JANET, in collaboration with partners from around the world.

Moonshot extends the federated identities advantages to a wide range of non-web services, including high performance computing, cloud and grid infrastructures and other non-web commonly services such as instant messaging, file storage or mail [3].

The Moonshot technology is the implementation of the IETF's Application Bridging for Federated Access Beyond web (ABFAB) [4] standards and makes use of EAP/RADIUS [5, 6] for authentication, as used in eduroam [7] and SAML [8] authorisation, as used in eduGAIN [9]. Moonshot specification allows a Moonshot IdP (Moonshot Identity Provider) to retrieve user attributes from a SAML IdP or an LDAP directory. The recovered information is sent by the Moonshot IdP to the SP in a standard SAML assertion.

2.1.1 Entities and architecture

Moonshot defines four main components (see Figure 3) to represent all the elements involved in its architecture. The interaction topology for these elements depends on the AAA architecture behind, but in general it should be hierarchical as classic RADIUS networks. Below is the description of the entities involved:

- Client: the end user's software installed on her computer and used for interacting with the service. The software allows the session to be started with the service and completes the authentication process at the IdP.

- Relying Party (RP): it consists of the service itself and the specific Moonshot module named Relying Party Proxy (RPProxy. It is a RADIUS server which allows the interconnection with the IdPs through the Trust Infrastructure (TI). During a new session, the Service part contacts the local RP Proxy, which uses its TI to find and forward the authentication request to the home IdP.

- Identity Provider (IdP): is the entity in charge of providing identity information about organisation members. The end user and IdP interact through RADIUS EAP secure tunnelling [3], which allows the obfuscation of user credentials for any intermediate party. After successful authentication, the IdP generates a SAML response with the success status and user's attributes, and sends it to the RP through the TI.

- Trust Infrastructure (IT): it is managed by the NREN and make possible the trust relationship between the RP and IdP. There are several possible configurations for the TI based on the communication path between both endpoints (RP and IdP). On one hand there is the classical hierarchical

RADIUS network (i.e. eduroam structure), on the other hand, it is possible the use of Moonshot Trust Router Network that allows direct communication between the Relaying Party and the Identity Provider, without pass through other proxyRADIUS servers.

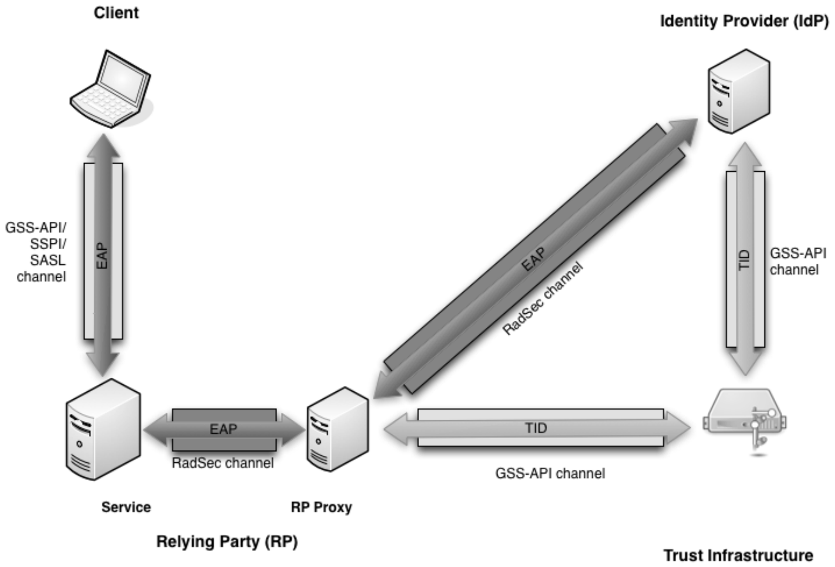

Figure 3: Moonshot architeccture [3].

2.1.2 Interaction flow

The steps of the protocol flow to access an OpenSSH service are as follows [10]:

1. The application client attempts to connect to the OpenSSH application server, using the application's standard protocol.

2. The client and the application server agree on the use of GSS-API authentication, so the client's device calls the GSS-EAP.

3. The GSS-EAP module requests user credentials for the service.

4. GSS-EAP mechanisms is agreed to be used as authentication mechanisms from the GSS-APi.

5. The client creates an EAP request using its GSS-EAP module, with the NAI anonymized version. A GGS channel is established and used to send the EAP message to the server.

6. On the server, a RadSec/RADIUS connection is open by the GSS-EAP module to its configured RP Proxy in order to send a RADIUS Access-Request message with the client's EAP message. On the application server, GSS-EAP could also create a SAML authentication request to be added to the RADIUS Access-Request.

7. The RP Proxy receives this request. Depending on the realm, it finds the IP of the IdP associated. With this, it can contact the IdP and interchange the keying material necessary to open a secure connection. The RP Proxy opens a RadSec/RADIUS connection, through which it forwards the RADIUS Access-Request with the encapsulated EAP message.

After this step, a secure tunnel exists between the RPProxy and IdP and also there is a path between the client and its IdP.

8. Using the EAP path between the client and the IdP, both choose the EAP method to use, in order to create a secure tunnel between them.

9. IdP and Client have to agree the EAP method to verify the credentials. In addition, a channel bindings message is send by the Client with the GSS name of the RP.

10. The IdP authenticates the client credentials and checks the GSS name. Then, EAP messages are exchanged so that the client and the IdP both end up with a copy of the EAP Master Session Key (EAP MSK) and EAP Extended MSK.

11. The IdP sends a RADIUS Access-Accept message with the encapsulated EAP success message to the RP Proxy with a, the EAP MSK, and possibly a SAML assertion.

12. The RP Proxy evaluates the user in function of its policies and the information retrieved from the IdP. In case of successful decision, the RP Proxy forwards the Access-Accept with an EAP positive response, EAP MSK, and possibly SAML assertion to the application server over the RadSec/RADIUS connection.

13. On the application server, the GSS-EAP module checks the EAP keys and, based on this information, it evaluates the user's access to the service. If it is positive, the server provides access to the client application.

2.1.3 Protocols and technologies

Moonshot uses different technologies and protocols to implement the ABFAB architecture. The authentication process is done using EAP/RADIUS and the authorisation information is interchanged using SAML.The end user's Client needs to be compatible with them in order to interact with the architecture. Therefore, Moonshot Project offers a GSS-EAP mechanism that allows the use of GSS-API authentication mechanisms in the EAP and RADIUS network. The support of GSS-EAP mechanism enables software to use Moonshot technology as an authentication and authorisation option. As alternative, there are SSPI and Security Support Providers (SSPs), which require the EAP-SSP module to allow the use of of SSPI-enabled by applications. Finally, another popular and compatible security protocol is Kerberos that acts as a mechanism for GSS-API and is supported by quite a few applications.

2.1.4 Audience and scope

Moonshot is general-purpose technology to built on and unify existing infrastructures (i.e. eduroam) and identity federations components (IdPs) with the aim of offering new services and possibilities based on them. Besides, it allows to be used on several scenarios with independence of a the audience.

The unifying feature allows fewer usernames and passwords for the user. It offers SSO to all of the services, with more secure authentications provided by the user's home organisation. In addition, it preserves user privacy by not releasing personally identifiable information - unless the user gives consent.

From the point of view of service administrators, Moonshot reduces the cost and effort of credential management, since the authentication and maintenance work is delegated to IdPs. At the same time, it allows flexible authorisation, since the service can manage the access control on the basis of user attributes.

2.1.5 Summary

Moonshot is a Jisc project that promotes the development of a single unifying technology to extend the benefits of federated identity to a broad range services beyond the web. Its ABFAB technology makes use of common security mechanisms and protocols such as SAML, GSS-API, EAP, Radius or AAA. Moonshot is general-purpose technology that allows fewer usernames and passwords for common users. From the administrators' point of view, it reduces the cost and effort of credential management, since it allows the authentication and maintenance work to be delegated to IdPs.

2.2 eduGAIN

The eduGAIN project (EDUcation Global Authentication INfrastructure) [9] has its origins as a research activity in project GEANT2 (2004-2009), co-funded by the European Union and today it interconnects identity federations around the world in the field of global research and the education community, simplifying access to content, services and resources. eduGAIN infrastructure allows the trustworthy exchange of identity information related to authentication and authorization infrastructure (AAI). An example of its architecture is shown at Figure 4.

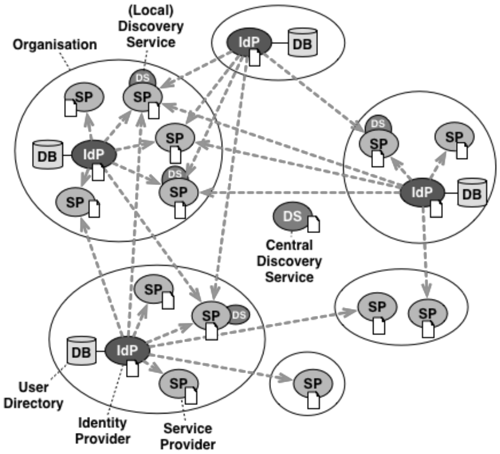

Figure 4: eduGAIN federation schema [11].

Thanks to eduGAIN, the IdPs can provide a wider range of services to their end users within an environment composed of multiple collaborative federations; The SPs can provide their services in different federations, amplifying their market possibilities; on the other hand, end users see increased service offering with security and trust. The Interoperable SAML 2.0 Profile (SAML2Int) [12] is the only SAML 2.0 profile allowed in eduGAIN.

2.2.1 Entities and architecture

eduGAIN architecture offers different possibilities [11] in relation to the topology configuration. In general, it follows a distribute topology but there are several options from full distributed to centralized: full mesh, hub & spoke with distributed login and hub & spoke with centralized login.

Below is the list of the main eduGAIN entities [13] involved in an standard interaction flow:

- Service Provider (SP): this component controls the user access to services and resources. It evaluates the assertion generated by IdPs and uses the information recovered to authorize access to protected services.

- Identity Provider (IdP): this entity is in charge of authenticating users and providing authentication and attributes statements about users to the requesting providers
- Discovery Service (DS): offers the user the possibility to indicate her Home Organization (HO) from a list to redirect her and thus to delegate her authentication to its HO's IdP.
- Metadata Distribution Service (MDS): metadata files collect technical data and descriptive information about the IdPs and SPs. The MDS aggregates and validates upstream metadata delivered by the participating federations. Furthermore, it signs and republishes the gathered metadata for consumption by the member federations, playing the role of central trust point. Individual SPs and IdPs should not consume the eduGAIN metadata directly.

2.2.2 Interaction flow

The typical eduGAIN login flow is described :

1. The user try to access a web SP.
2. The SP requires user authentication so it redirects her to the DS in order to select her home IdP. Often the DS can be deployed with the SP or offered by the SP itself.
3. With this information, the SP redirects the user to her IdP with an authentication request.
4. At the IdP, the user is authenticated by introducing her credentials, based on this, the IdP generates a SAML assertion with the result of the process and user information and redirect her again to the SP with a SAML response.
5. Based on the information received, the SP verifies the user identity information and authorizes access to the service.

2.2.3 Protocols and technologies

eduGAIN federations are based on SAML2INT. This specification defines an interoperable subset of SAML 2.0 protocol [1] that guarantees the interoperability. The SAML 2.0 WebSSO INTeroperability Deployment Profile defines a minimum set required to be followed by entities participating in eduGAIN with regard to which bindings should be used, which parts of the SAML messages should be signed or encrypted and how, rules, etc.

As regards specific software, most of the eduGAIN deployment is based on Shibboleth [14]. The Shibboleth Internet2 middleware Project propose an architecture for identity management and federated identity-based AAI (Authentication and Authorization Infrastructure). It also offers an open-source implementation of this architecture based on SAML2.0. Due to this, its software fits perfectly with the eduGAIN requirements so its SP and IdP software are widely used in eduGAIN environments.

2.2.4 Audience and use scope

eduGAIN project was designed to interconnect identity federations around the world in the field of global research and the education community. Its main promoters are the NRENs, which are part of GÉANT, but currently it is extended to Universities and research centers around the World and joins up 40 federations.

eduGAIN allows students, researchers and educators to access online services while minimizing the number of accounts users and service providers have to manage, which reduces the costs, the complexity and the security risks. In addition, it offers SPs access to a larger pool of international users, and makes access to resources of peer institutions or commercial or cloud services available to users using their one trusted identity.

2.2.5 Summary

The eduGAIN initiative is co-funded by the European Union and today interconnects identity federations around the world. It makes possible the trustworthy exchange of identity information related to AAI. It is based on SAML 2.0 Interoperable Profile, a subset of the SAML2.0 standard focused on easing the interoperability. eduGAIN was designed from its beginnings to interconnect global research and educational centers, and its main users are students, researchers and educators.

2.3 EUDAT

The EUDAT project [15] is a pan-European data initiative that had a first stage between 2011-2014 and was extended in 2015 to run till 2018. The project started with a single consortium of 25 partners, including cooperating centers, thematic data centers and some of Europe's largest scientific data centers. It aims to support multiple research communities offering common data services, building a sustainable cross-disciplinary and cross-national data infrastructure that provide a set of shared services for accessing and preserving research data [16].

The AAI component of EUDAT is B2ACCESS [17]. It is an easy-to-use and secure AAI that can be integrated with different services, allowing users to log in with varied authentication methods (OAuth2, SAML, X.509 SLCs). When the user authenticates for first time, she creates a new EUDAT ID in the B2ACCESS service using her home IdP (e.g. Facebook, Google, eduGAIN, X.509, etc.). The use of user's home IdP (external) is the recommended way to interact with EUDAT. In addition, B2ACCESS offers a range of tools and services to manage, store and share data (B2SHARE, B2SAFE, B2DROP, B2FIND, etc.).

2.3.1 Entities and architecture

EUDAT architecture bases its operation on B2ACCESS services that centralize all identity services. In contrast, it offers the possibility to replicate and distribute some services to adapt to the needs of the organizations that implement it. The entities involved and their functions are depicted in Figure 5 and described below:

- Service Providers: these entities, also called Downstream Services, offer services protected by the EUDAT architecture. When a user accesses to the SP, it requests attribute assertions generated by the B2ACCESS service.

- Primary Identity Providers: these are external IdPs that provide identities and attributes using different technologies such as OpenID, SAML or X.509.

- B2ACCESS AAI Functions: the Unity IdM component of the B2ACCESS service maps recovers information from the Primary Identity Provides onto an EUDAT identity. The role of B2ACCESS is to provide user authentication and authorisation assertions to the SPs,.B2ACCESS can play the IdP role and authenticate its own users, using a specific EUDAT username and password.

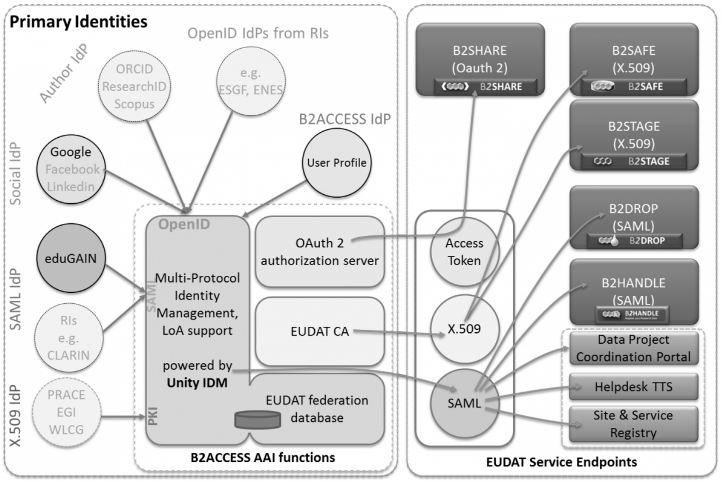

Figure 5: EUDAT internal architecture based en B2ACCESS [17]

- EUDAT Service Endpoints: These tools are responsible for managing, storing and sharing user data from the EUDAT identity.

2.3.2 Interaction flow

Due to the flexibility offered by the authentication methods, the flow will vary to suit the chosen mechanism. The login flow example described below is taken from [18] and corresponds to the SAML IdP scenario:

1. The end user wants access an EUDAT service that offers a protected resource (e.g. B2SHARE)

2. The user is not authenticated so she is redirected to B2ACCESS.

3. The B2ACCESS make possible to select from a list the user's home organisation IdP.

4. Based on IdP selection, the user is redirected to her IdP login page, where she is authenticated with her credential.

5. In case of successful authentication, the user is redirected to the B2ACCESS with the authentication message from the IdP.

6. The end user is redirected to the SP by the B2ACCESS service with the EUDAT identity and attributes in the format used to integrate the service (i.e. OAuth2).

7. Then, the SP decides if the user is authorised or not in function of the information retrieved from B2ACCESS.

2.3.3 Protocols and technologies

EUDAT is able to work with several authentication protocols such as: SAML2.0, OAuth2, X.509 certificates. It makes interaction with other federation systems like eduGAIN, Google or Facebook possible. The B2ACCESS identity management software makes use of Unity Project [19], which offers "a complete solution for identity, federation and inter-federation management" [20]. It enables the authentication process using various protocols, with different configurations. Internally, Unity is composed of an orchestration platform with highly specialized extensions that provide support for the actual Unity features. The sources and binaries are protected by copyright, but it allows their redistribution and use under the same conditions and rights.

2.3.4 Audience and scope

EUDAT consortium involves 36 European Partners, being more than half Computing and Data Centers [21]. Its target audience are citizen scientists and,staff and users from science organisations, research institutions and universities, being managed by community data managers. Some deployment examples listed at [22] are: EPOS (Earth observation), ENES (climate), VPH (bio-medical sciences), ICOS, LTER and. CLARIN (linguistics),

2.3.5 Summary

The EUDAT project is a pan-European initiative formed by 36 partners. Its architecture is based on B2ACCESS AAI services and a complete set of backend services and tools to manage, store and share data (B2SHARE, B2SAFE, B2DROP, B2FIND, etc.). As it is based on Unity IdM software, EUDAT is able to work with several authentication protocols such as SAML2.0, OAuth2 and X.509 certificates, which allows interaction with several identity federations. The project work is oriented to Computing and Data Centers.

2.4 STORK

Secure idenTity acrOss boRders linKed 2.0 (STORK 2.0) is carried out by 19 EU/EEA Member States and 59 partners of different types, such as governmental institutions, banks or universities [23]. The initiative works to offer citizens a single European electronic identification and authentication zone in collaboration with public and private service providers that allow establish new electronic relations between citizens and foreign e-services. This pilot experience has also contribute to elaboration of the eIDAS normative, which will be reviewed in the next section.

STORK has implemented security guidelines and requirements [24] that all countries involved have to adhere to, being one of its most relevant characteristics the high level of assurance (LoA) offered and required in the authentication process, which is delegated into each Member State.

Its architecture is defined as a user centric system, so users must maintain the control of information shared with an entity, the specific origin and destination of their information. The user must be informed of the context, the sector (government, public, health, . . .), the privacy or data usage policy, the liability disclaimer or any other aspect of each country's legislation where her informations will be used and gives her consent The user's personal information revealed to an entity should be the minimum needed for the purpose of the service provided.

2.4.1 Entities and architecture

STORK architecture (Figure 6) has a hybrid topology based on the interaction between the PEPS and the rest of entities. By each country, STORK has one PEPS that acts as centralized point for all the users, Services Providers and Identity Providers of this country. In contrast, the topology between the PEPS is full distributed, with one-to-one trust relationships. This architecture allows that each country can maintain the control of what users and services providers are connected within its borders, while managing relations with the rest of the countries.

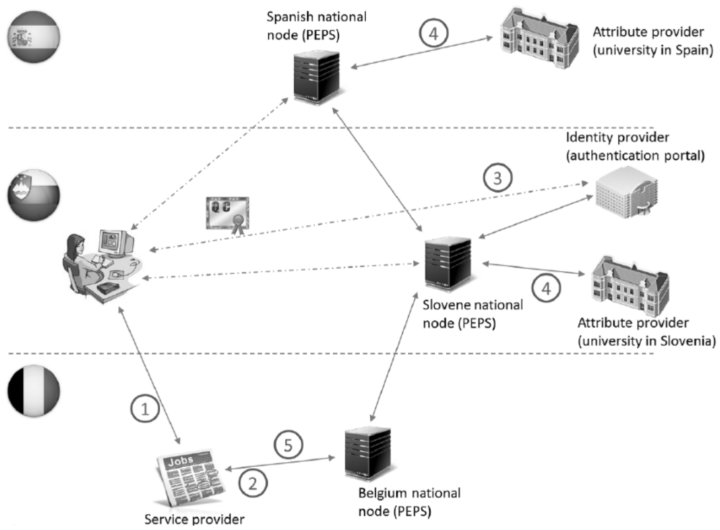
Spanish national node (PEPS)
4
Attribute provider (university in Spain)
Identity provider (authentication portal)
3
Slovene national node (PEPS)
4
Attribute provider (university in Slovenia)
1
5
2
Service provider
Belgium national node (PEPS)
Jobs

Figure 6: STORK 2.0 infrastructure example [25].

As detailed below, this is the list of main STORK entities involved in a standard interaction flow:

- PEPS (Pan European Proxy Server): Each PEPS includes the functionalities which are specific to its Member State, which are typically the interfaces with the local ID providers, domain-specific attribute providers and mandate providers. It plays two principal roles: the S-PEPS (Service PEPS) that attends SP and forwards it to her colleague PEPS or V-IDP and the C-PEPS (Citizen PEPS), which attends to citizen requests and resolves the requests received from her colleague PEPS or V-IDP.
- IdP (Identity Provider): this is responsible for managing and issuing identity information to service providers and doing the authentication.
- AP (Attribute Provider): this entity stores user attributes and returns them to the PEPSes
- SP (Service Provider) offers a protected resource or application to the user and usually initiates an authentication.

2.4.2 Interaction flow

The typical STORK 2.0 flow is described below:

1. Spanish STORK user tries to access a STORK SP that depends on the Italian infrastructure
2. The user indicates her country of origin in order to be authenticated by her home IdP. With this information, the SP redirects the user to the Italian S-PEPS.
3. The Italian S-PEPS uses the country information to redirects the user to her origin C-PEPS, in this case, the Spanish PEPS.
4. The Spanish C-PEPS requires explicit user consent prior to requesting her authentication and the requested attributes.

5. If the user agrees, she is redirected to the IdP, where she is authenticated using her national eID. The IdP requests the user's consent to share the requested attributes with the C-PEPS.

6. The Spanish C-PEPS redirects the user back to the Italian S-PEPS and the latter back to the SP. The PEPS's response includes the authentication statement and the user attributes.

7. Based on the information retrieved, the SP evaluates them and decides whether to grant the user access to the service.

2.4.3 Protocols and technologies

The protocol implemented in STORK 2.0 is called SAMLSTORK, which has been designed as a subset of SAML2.0 standard with some extensions [26]. The SAML's extension capability has the advantage of allowing the customization of communication protocol and the transport of specific attributes. It makes it possible, among other functions, to request and transport specific information and attributes required by STORK such as QAA and AQAA. In contrast, the use of these extensions make direct interaction with other pure SAML systems impossible.

2.4.4 Audience and scope

STORK 2.0 is divided into four areas of interest: eLearning, eHealth, eBanking and Public Services for Business, which are considered the most interesting to promote the use of the European eID. The pilot involves partners from all these areas, with the participation of end users, service providers and European Member States. In fact, STORK has as its target the whole European Union, its citizens and all the SPs that in one way or another want to take advantage of the STORK infrastructure and the security features it offers.

2.4.5 Summary

STORK 2.0 is a pilot based on the STORK project and carried out by 19 European Member States and 59 partners of different types, such as governmental institutions, banks or universities. The initiative was planed with the aim of being helpful in the preparation of the eIDAS regulation. STORK offers and requires high levels of security and privacy to users and services due to work at governmental levels. It is based on SAMLSTORK, which uses SAML extension capabilities to introduce new attributes and custom information. These modifications and the security restrictions make STORK incompatible with other standard SAML federations.

2.5 eIDAS

eIDAS Regulation [27] on electronic identification and trust services for electronic transactions in the European internal market is based on the work done along the STORK and STORK2.0 projects and it has been designed as an evolution of both of them. It was published in regulation N^{o}910/2014 and adopted by the co-legislator on July 2014 The European normative obliges all Member States to become eIDAS compliant in 2018, thus enabling recognition of the notified e-ID means.

It offers a regulatory environment that guarantees people and services the use of their national electronic identifications (eIDs) to use public e-services in all European countries where the eIDAS is already available, so encouraging the creation of an European internal market for electronic Trust Services (eTS) and ensuring across border works, with the same legal reliability as traditional face to face or paper based procedures. Indeed, one of the main objectives is to make disappear the existing barriers to the electronic identification between citizens and services from different Member States using the eIDAS cross-border authentication for at least public services.

2.5.1 Entities and architecture

Like STORK, eIDAS has a hybrid topology based on the previous STORK architecture. By each country, eIDAS has one eIDAS Node that acts as centralized point for all the users, Services Providers and Identity Providers of that country. At European level, all eIDAS nodes are organized in a distributed topology that allows that each country can maintain the control of what users and services providers are connected within its borders, while managing fine grain control in the relations with the rest of the countries.

The entities involved in eIDAS architecture [28] are described below:

- Member State: State covered by the eIDAS regulation. It acts as Sending MS when it is in charge of authenticating the eID scheme and sending the ID data to the Receiving MS. In contrast, it acts as Receiving MS when one of its Relying Parties requests the authentication of a person through it.
- Relying Party (RP): this entity represents any natural or legal person, in general it is a service provider, that requires an electronic identification of a citizen or a trust service in order to provides a service.
- eIDAS-Node: it is an operational entity involved in cross-border authentication of persons. A Node can have different roles, which are distinguished in this specification (eIDAS-Connector/eIDAS-Service, see below).
  - eIDAS-Connector: an eIDAS-Node requesting a cross-border authentication.
  - eIDAS-Service: an eIDAS-Node providing cross-border authentication.
    - eIDAS-Proxy-Service: an eIDAS-Service operated by the Sending MS and providing personal identification data.
    - eIDAS-Middleware-Service: an eIDAS-Service running Middleware provided by the Sending MS, operated by the Receiving MS and providing personal identification data.
- eID Scheme: There are two options to provide the eID scheme according to the eIDAS-Service interface. The Proxy based scheme is a (notified) eID scheme which provides cross-border authentication via an eIDAS-Proxy-Service and the Middleware based scheme is a (notified) eID scheme which provides cross-border authentication via eIDAS-Middleware-Services

2.5.2 Interaction flow

This section describes the process flow to authenticate a person, enrolled in the eID-scheme of the Sending MS, to a relying party established in the Receiving MS [29].

1. A user tries to access a resource protected by the RP, which sends an authentication request to the eIDAS-Connector responsible for RP. The eIDAS-Connector can be directly attached to the RP (Decentralized MS) or operated by a separate entity (Centralized MS).
2. The eIDAS-Connector requests the MS in charge of authenticating the user on the basis of the eID scheme.

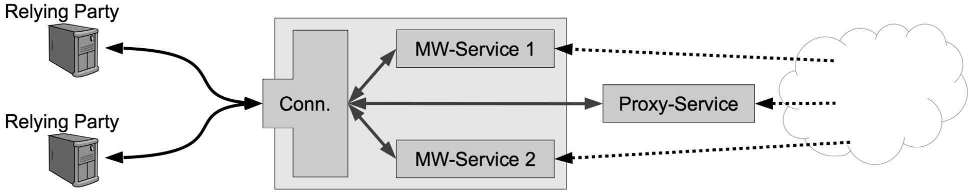

Figure 7: eIDAS components.

3. The eIDAS-Connector sends a SAML Request to the eIDAS-Service corresponding to the selected MS.

4. The eIDAS-Service must verify the authenticity of the Request and check the terms of access and the Level of Assurance (LoA) required in the request.

5. The eIDAS-Service performs the authentication of the person according to the selected eID scheme and sends back a SAML Authentication Response.

6. The eIDAS-Connector verifies the Response message authenticity and decrypts the Assertion. The Connector must verify the LoA and send the received authenticated person identification data to the requesting party

2.5.3 Protocols and technologies

SAML 2.0 is the base protocol to communicate and encode eIDAS information and messages. As in STORK, eIDAS uses SAML extension capabilities to customize the information transmitted and also to encode specific information.

The eIDAS Project also provides software to simplify the adoption by Providers and Member States. DG DIGIT provides an implementation of the eIDAS-Connector and the eIDAS-Proxy-Service as a single package licensed under the EUPL, under the CEF (Connecting Europe Facility) program. CEF Management Board manages the implementation requirements, including provisioning and service support. This implementation is provided bundled with the Middleware provided by the Member States.

2.5.4 Audience and scope

eIDAS, as an evolution of STORK, has is target audience in all the Member States of the European Union, including their citizens and public and private services related with government administrations.

The stakeholders of the eIDAS-Network are, in first place, the citizens, who expect confidentiality with their person identification data at the same time that they require the eIDAS-Network to respect their privacy. In the second place, there are the operators of components of the eIDAS-Network with requirements derived from the requirements of the relying party and the citizens. Finally, all the relying parties that require authenticity/integrity of the person identification data received with the aim of fulfilling the data protection obligations related to confidentiality and privacy.

2.5.5 Summary

The eIDAS Regulation was published in 2014 as a regulatory environment that guarantees people and services the use of their national eIDs to use public services in all European countries with the same legal reliability as traditional paper based procedures. eIDAS promotes and facilitates the use of cross-border electronic identification and trust services, and guarantees transparency and accountability. The regulation also contributes to the enhancement of trust and security of digital transactions and thus to the building of the Digital Single Market. The objective is to extend and popularize the use of eID among citizens of the European Union in their relations with institutions as well as in the private sector.

2.6 Identity Federation Summary

Table 1 summarizes of all the identity federations studied in this section, with the aim of offering an overview of their main characteristics.

	Moonshot	eduGAIN	EUDAT	STORK	eIDAS
Entities	Client, RP, IdP, Trust Infrastructure	SP, IdP, DS, MDS	SP, Primary IdPs, B2ACCESS AAI, EUDAT Service Endpoints	SP, PEPS (S-PEPS & C-PEPS), IdP, AP	RP, eIDAS Node, IdP
Topoloy	Hierachical	Distributed	Centralized	Hybrid	Hybrid
Protocols	EAP/ RADIUS, SAML2	SAML2	SAML2, OAuth2, X.509, …	SAMLSTORK	SAMLSTORK
Software	GSS-API, SSPI Kerberos	Shibboleth	B2ACCESS (Unity)	Demo software for SP, PEPS, IdP& AP	Demo software for RP, Nodes, eID Scheme
Audience	general-purpose	Researchers, students, university staff	Researchers	European citizens	European citizens
Scope	general-purpose	Research centers, universities	Research and data centers	eLearning, eHealth, eBanking, Public Services for Busines	Public administrations, public and private services
Countries involved	Global	Global	Europe	Europe	Europe

Table 1: Identity federations summary.

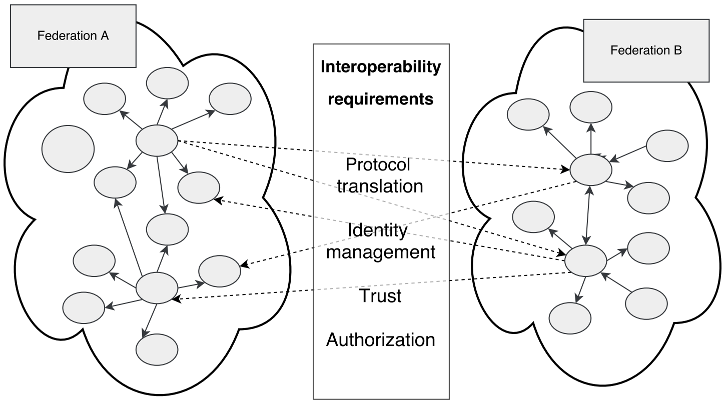

Figure 8: Interoperability requirements for existing federations.

3 Federation Integration: Possibilities

As we have seen in the previous section, multiple identity federations systems have emerged in recent years. Most of them are based on SAML protocol to encode and transmit the identity information, but this does not guarantee the interoperability between them, due to distinctive features that prevent the interaction between federations. In general, deployed federations are isolated from others, users need specific credential to access to each one and services are limited to its federation's audience.

There are projects focused on promoting the integration of new services such as eduGAIN and EUDAT, but the problem persists in the case of deployed federations that have been successfully adopted and can not be directly integrated.

The interconnection of identity federation is a relevant work area with several project and researchers working in parallel. A very important work is being done in papers like [30] and the LIGO Project [31] to analyse the requirements of federation and interfederation initiatives and propose alternative solutions to solve the problem like the GÉANT Trust Broker [32]. Kantara initiative [33], which is based on Liberty Alliance Identity Assurance Expert Group [34], works on create a common framework to harmonize baseline policies, business rules, and commercial terms against which identity trust services can be assessed and evaluated. Other projects, like InCommons [35] in the United States and AARC [36] in Europe, dedicate part of their efforts to expand their base federations to interconnect with others.

An interoperability solution has to offer mechanisms to solve different aspect related to protocol interoperability, identity management, trust and access control (authorization mechanisms) as it is depict in Figure 8. The use of existing interfederation solutions to interconnect deployed federations imply the migration or adaptation of operating production services to new authentication and interoperation mechanisms. In some cases, as for example new deployments, it can be a good option, but when the work have to be done with running federations and services, it might not be a practical option because, in general, it entails the modification of entities involved and user interaction flows. The complexity is even greater when the proposed solution involves using OAuth [37, 38] or OpenID Connect [39] as authentication and authorization protocols instead of SAML, since it involves migration to the new protocols or the bidirectional translation to SAML. Other solutions based on SAML like Shibboleth [40] imply the adoption of a complete new layer with a consequent increase in operation complexity, rules and political agreements management. These reasons lead to the design of an ad-hoc solution to resolve the specific problems of integrating these particular federations minimizing the number of added elements and modifications.

The establishment of interoperability mechanisms can allow transparent interaction for services and users from different federations thanks to the integrations of their identity management mechanisms and trust control. An optimal integration can also allows users to maintain their identities between federations and, at the same time, access to services of the other federation. There are many desirable features in the integration of existing federation related to different aspects:

- Transparent integration: This feature is one of the most important and can determine if an interoperability solution is adopted or not. It makes reference to how the integration affects to users, service providers and identity providers. In function of how many entities have to be involved in the integration process and how much, learning new procedures to solve the same use case (users) or new emerging use cases, modifying their configuration files or even their source code (providers), changing their privacy and security policies (service and identity providers), between other possibilities. Insofar as integration is more transparent and affects fewer entities, the integration process will be simpler, faster, cheaper and more comfortable, and therefore with more chances of adoption and success.

- Identity matching: the use of services and resources from one federation for users of the others is the final objective of the integration process, but when we talk about the integration of existing federations it is necessary to consider the possibility that an user already has accounts created in both federations. The establishment of mechanisms that allow linking both digital identities, if the user so wishes, is a very interesting and desired feature that offers an improved user experience. This feature can be difficult to achieve, even more if you try to provide in a transparent manner.

- Trust relationship: in the integration process will be necessary to establish new trust relationships between the entities involves. In function of how are initially established the trust relationships in the federations (by the topology and the internal architecture) and the integration solution proposed, more o less entities will be involved in the process and required to create new trust agreements. In some cases, it is possible to maintain the trust control at federation level, which greatly simplifies the creation and management of new trust relationships.

- Privacy and security: user privacy is a key factor for the integration process. Depending on how is designed the interoperability solution, each federation can maintain the control of their users data or maybe, they can share and mix their users database. In addition, the integration of users and services requires studying and comparing privacy policies, with the aim of keeping the security and privacy levels offered to the users by original federations. In case of finding differences, the integration solution should work on guarantee the higher level of security and the more restrictive privacy policies.

- Live migration: another desirable feature in relation with design an interoperability solution for existing and running federations is the possibility of offering the integration with long cuts in services. This feature is closely related to the transparency and security of the proposed solution.

The ideal objective in the interfederation problem of two existing identity federations is to achieve bidirectional matching between identities with the specific properties of transparent, fluid and “on the fly” integration between users and services of both federations, not only allowing basic authentication but also complex scenarios like linking existing accounts and requesting additional attributes to provide identity management. To reach total integration for all the use cases is a very ambitious objective and requited the study of different integration possibilities depending of the preconditions and the scenarios proposed. In order to define and interoperability solution between two federations, it is necessary to define the equivalence between entities and all the required mechanisms to translate and do the matching between identifiers, messages and protocols.

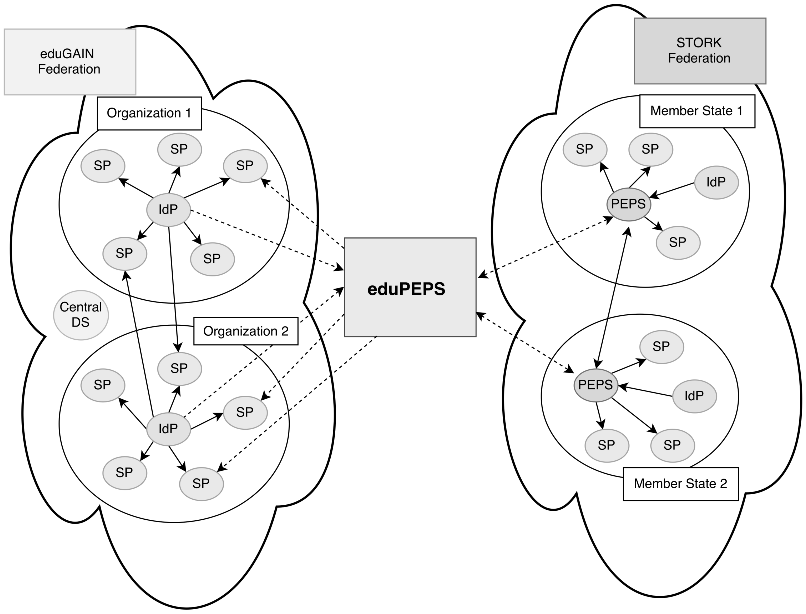

Figure 9: eduGAIN and STORK interfederation through eduPEPS.

Some identity federations like STORK and eIDAS were born as federations with very specific and strict requirements in security and trust areas and are focused on keeping control in the hands of the end user at all times. The integration of this kind of federation requires additional and specific work focusing on solving technical interoperability gaps and political and legal issues required to reach a real interoperation. Their interconnections with eduGAIN are particularly beneficial since, while their initial scopes are different (public institutions vs educational sector), the integration of their users and services has an enormous potential interest for both since, on the one hand, there is a great potential to increase the number of users, and on the other, it is possible to offer a large number of new services that were not included initially. Besides, the high level of security required in STORK and eIDAS means eduGAIN can take advantage of it to improve the LoA offered to its services. All these factors promote the interest from GÉANT and from the European Commission to establish the necessary interoperability mechanisms to achieve this.

The following sections offer interoperability solutions between eduGAIN and STORK and eduGAIN and eIDAS. Our proposal focuses on offering a tailor-made solution that enables both federations to be integrated without having to migrate entities to new protocols, modify deployed services while supporting end user interaction flows as much as possible.

3.1 eduGAIN and STORK

As commented on earlier, eduGAIN is the federation par excellence in the educational and research sector around the world, especially in universities and research centers. In contrast, STORK is focused on governmental services and institutions inside the European Union. Although STORK is based on SAML2.0, it implements some extensions that together with some particularities, such as the identifier and attributes used and its rigid infrastructure based on PEPS, make direct interconnection with eduGAIN federation impossible.

Both federations have entities in common with almost equal functions, such as users, SPs, IdPs and APs,. The problem comes with intermediary entities like STORK's PEPS and eduGAIN's MDS that

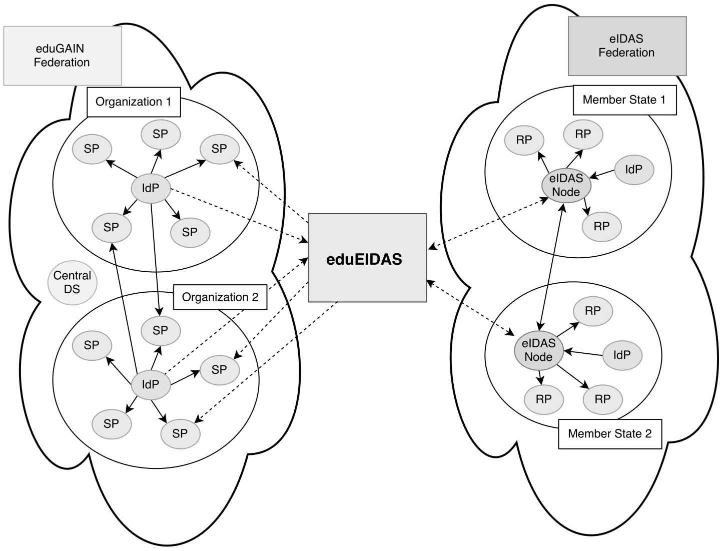

Figure 10: eduGAIN and eIDAS interfederation through eduEIDAS.

have not got a direct match. STORK PEPS plays different roles depending on the entity with which it has to interact. When it plays the role of S-PEPS, it shows the list of available C-PEPS to the user so that she can choose her national PEPS. At the same time, eduGAIN offers a similar functionality through the WAYF Service (Where Are You From). In the second role, the C-PEPS redirects the citizen to the official IdP and allows her to choose which attributes have to be recovered in each IdP and AP. In eduGAIN, this functionality could be done by the IdP, the DS or even statically.

The proposed solution is to incorporate a new entity, denominated eduPEPS, situated between the STORK and eduGAIN federations. This entity, that was presented in [41] would be in charge of the SAML translation (between SAMLstork and SAMLint) as well as of the identifier and attributes translation. The eduPEPS have to act as a trusted entity for both federations, playing the role of DS and MDS of any other eduGAIN federation for the eduGAIN side, and acting as a PEPS (S-PEPS or C-CPEPS depending on the scenario) of another country for the STORK side.

The eduPEPS element allows us to incorporate the concept of Virtual Country for the eduPEPS from the STORK point of view. This perspective allows us to treat eduGAIN federation as if it were a virtual country. In STORK, each country needs legal agreements to be trusted by each national PEPS, therefore through this equivalence each STORK Member State can decide if allows the eduGAIN integration or not.

Regarding the case of eduGAIN users visiting STORK services, the eduPEPS would act as C-PEPS providing the user with a list of available eduGAIN federations and redirect her to the DS of the selected federation. There is the possibility of importing the metadata from eduGAIN MDS eduPEPS and directly offer the list of IdP.

3.2 eIDAS and eduGAIN

eIDAS, as an evolution of the STORK project, has similar peculiarities and problems to interact with eduGAIN. The differences in SAML dialects, identifiers and attributes, together with high security and legal requirement and restrictions make this impossible.

As with STORK, the introduction of a new intermediate entity (Figure 10) enables all technical problems of compatibility between federations to be solved. The new entity, named in this case eduEIDAS, also has to translate between SAMLINT and SAMLSTORK dialects, translate and do the matching between attributes and identifiers and act as trust point for both federations, so all the mechanisms and tools designed and developed for the previous integration scenario can be used as a base here.

In eIDAS, the central element of the architecture is the eIDAS Node, which has similar characteristics to the STORK PEPS. In general, the eIDAS Nodes is the central point of trust and interconnection of each Member State and is used as gateway in the cross-border operations. As we saw in eIDAS section, it has two different roles depending on whether it acts as Connector or Service Node.

In the case of an eduGAIN user accessing an eIDAS RP, the eduEIDAS plays the role of the Service Node from the point of view of eIDAS and acts as a SP that requests user authentication from the eduGAIN IdP. In the case of an eIDAS user accessing an eduGAIN SP, the eduEIDAS can play the role of DS and MDS and replace the IdP. From the point of view of eIDAS, it acts as Connector Node of the Receiving Member State.

eIDAS architecture also allows the use of Virtual Country concept introduced in previous scenario, which simplifies the trust management and allows selective adoption by each Member since in eIDAS each country needs legal agreements to be trusted by each national eIDAS Node.

3.3 Summary

Our proposal of introducing a new entity in both cases allows all the translation and interoperability work to be concentrated in a single point. This also greatly simplifies the new trust relationships that will need to be established between both federations, so facilitating the management of security and privacy. The proposed solution offers protocol interoperability thanks to the translation capabilities between SAML protocols. It also offers identity management since, trust and access control thanks to the interoperability mechanisms around the identity information making compatible the authentication process and allowing recover attributes between federations.

The benefits of STORK and eIDAS integration with eduGAIN are very significant. The huge increase in the number of users as well as new offers of services are the main drivers of integration. From the eduGAIN point of view, it gains a huge base of users that already have official eIDs and, in addition, the high LoA offered by eIDAS allows the replacement of face to face procedures. From the point of view of eIDAS, the interconnection with eduGAIN federations allows interconnection with users and services outside the European Union, which means extending the type and number of services and improving the relations with non European citizens.

4 Conclusion

People and services increasingly demand a greater interconnection to unite and offer common services as a way to win new users, improve existing ones and simplify the management. There exist a wide variety of identity federation systems according to the requirements of users, services and scopes, and the most active work in this IT area is being done by the research and administration sectors. The latest trends and advances focus not only on guaranteeing the user privacy and improving the security, but rather on enhancing the improvement of existing federations through their interconnection, which allows a larger user base, unified services and management, and creates a set of new services in line with the new possibilities.

In order to appreciate the intense work done in the area of AAI to improve the infrastructure used and the services deployed, this paper review some of the most relevant identity federations based on SAML. In first place we analyse Moonshot as a general purpose option, continuing with eduGAIN and EUDAT which are very important in educative and research sectors. Finally, the review places special emphasis on those options related to the Administration sector such as STORK and eIDAS. The review offers a general overview of the main characteristic of each federation.

Based on the identity federation analysis, we set out the problem of interconnecting federations in specific in scenarios where the federations are already deployed and running. Our work attributes the main problems to the differences in communication protocols, attributes sets and identifiers as well as to the differences found in security restrictions and requirements. The interoperability between federations offers a wide range of benefits from the huge increase in users, to the creation of new services and the improvement of existing services to the security upgrade. The definition and implementation of interoperability mechanism and is critical for the successful advancement of digital technologies.

The first interoperability case studied involves eduGAIN and STORK federations. Migrating from one federation to other or establishing a complete new interoperability layer between both of them is not practical, due to the size and level of deployment. Although both federations are based on SAML, the modifications introduced by STORK make it impossible to integrate from a low level. We propose as a solution the incorporation of a new customised intermediate entity, the eduPEPS, which is in charge of translating between SAML dialects, translating attributes and identifiers. The eduPEPS has to offer interfaces with STORK and eduGAIN entities, acting as trust central point for both federations and simplifying the management of interfederation process.

This solution can be extrapolated to the integration between eIDAS and eduGAIN. Although eIDAS is based on STORK, eIDAS has its own characteristic that requires a personalized solution. In this case, we propose the incorporation of a new entity, called eduEIDAS that has to play the role of eIDAS node and eduGAIN's MDS, DS and WAYF services. Thanks to the translation mechanisms of the eduEIDAS, all the technical interoperability gaps can be solved

Identity federation interoperation allows better privacy and security control of user personal data, improving and simplifying the management and the interaction with service providers. Public administrations are relatively new actors in the IT world, with great potential to harmonize existing federation, with the guarantee of being able to offer high quality information for services and at the same time maintain the utmost respect for the privacy of users.

Acknowledgments

This paper has been also possible partially by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2). Authors also thank the Funding Program for Research Groups of Excellence with code 04552/GERM/06 granted by the Fundación Séneca and the Spanish National Project CICYT EDISON (TIN2014-52099-R) granted by the Ministry of Economy and Competitiveness of Spain (including ERDF support).

References

[1] S. Cantor, J. Kemp, R. Philpott, and E. Maler, "Assertions and Protocols for the OASIS Security Assertion Markup Language SAML V2.0 SAML Core," 2005, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, [Online; Accessed on June 1, 2017].

[2] A. Perez-Mendez, F. Pereñígez-García, R. Marín-López, G. López-Millán, and J. Howlett, "Identity federations beyond the web : A survey," *Journal of IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2125–2141, May 2014.

[3] Moonshot, "Moonshot WIKI," 2015, https://wiki.moonshot.ja.net/, [Online; Accessed on June 1, 2017].

[4] J. Howlett, S. Hartman, H. Tschofenig, and J. Schaad, "Application Bridging for Federated Access Beyond Web (ABFAB) Architecture," IETF RFC 7831, May 2016, https://datatracker.ietf.org/doc/rfc7831/, [Online; Accessed on June 1, 2017].

[5] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz (Ed.), "Extensible authentication protocol (eap)," IETF RFC 3748, June 2004, https://tools.ietf.org/html/rfc3748, [Online; Accessed on June 1, 2017].

[6] A. DeKok and A. Lior, "Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions," April 2013, https://tools.ietf.org/html/rfc6929, [Online; Accessed on June 1, 2017].

[7] "eduroam Portal," https://www.eduroam.org/, [Online; Accessed on June 1, 2017].

[8] N. Ragouzis, H. Lockhart, B. Campbell, N. Ragouzis, H. Lockhart, B. Campbell, N. Ragouzis, H. Lockhart, and B. Campbell, "Security Assertion Markup Language (SAML) V2.0 Technical Overview," March 2008, https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf, [Online; Accessed on June 1, 2017].

[9] "eduGAIN Portal," 2016, http://services.geant.net/edugain/Pages/Home.aspx, [Online; Accessed on June 1, 2017].

[10] R. Smith, "The Architecture and Protocol Flows of Moonshot," 2014, https://wiki.moonshot.ja.net/display/Moonshot/The+Architecture+and+Protocol+Flows+of+Moonshot, [Online; Accessed on June 1, 2017].

[11] T. Baerecke, "Federation Architecture," 2014, https://wiki.edugain.org/Federation{_}Architecture, [Online; Accessed on June 1, 2017].

[12] SAML2int, "saml2int - The Interoperable SAML 2.0 Profile," 2015, http://saml2int.org/, [Online; Accessed on June 1, 2017].

[13] eduGAIN WIKI, "eduGAIN WIKI Therminology," 2014, https://wiki.edugain.org/Terminology, [Online; Accessed on June 1, 2017].

[14] Shibboleth, "Shibboleth Project," 2012, http://shibboleth.net/, [Online; Accessed on June 1, 2017].

[15] D. Lecarpentier, P. Wittenburg, W. Elbers, A. Michelini, R. Kanso, P. Coveney, and R. Baxter, "EUDAT: A New Cross-Disciplinary Data Infrastructure for Science," *International Journal of Digital Curation*, vol. 8, no. 1, pp. 279–287, 2013.

[16] D. Lecarpentier, A. Michelini, and P. Wittenburg, "The building of the EUDAT Cross-Disciplinary Data Infrastructure," http://adsabs.harvard.edu/abs/2013EGUGA..15.7202L, [Online; Accessed on June 1, 2017], April 2013.

[17] EUDAT, "B2ACCESS Project webpage," 2016, https://eudat.eu/services/b2access, [Online; Accessed on June 1, 2017].

[18] L. Hämmerle, R. Sabatino, T. Lenggenhager, M. Mantovani, P. Pilt, L. Toom, L. Jensen, E. Torroglosa, S. Paetow, P. Solagna, W. Elbers, A. Ceccanti, B. Wegh, M. Hardt, P. Millar, and J. Reetz, "GN4 - 1 White Paper : Comparison of Authentication and Authorisation Infrastructures for Research," 2016, http://www.geant.org/Resources/Documents/Comparison-of-AAIs-for-Research_White-Paper_v1.0.pdf#search=edugain, [Online; Accessed on June 1, 2017].

[19] Unity, "UNITY - Identity relationship managment." 2017, http://www.unity-idm.eu/, [Online; Accessed on June 1, 2017].

[20] Unity Team, "Unity Manual Version 1.9.4," 2016, http://www.unity-idm.eu/documentation/unity-1.9.4/manual.html, [Online; Accessed on June 1, 2017].

[21] EUDAT, "EUDAT Partners," 2017, https://eudat.eu/partners, [Online; Accessed on June 1, 2017].

[22] EUDAT Project, "EUDAT Use Cases," 2016, https://eudat.eu/use-cases, [Online; Accessed on June 1, 2017].

[23] STORK-eID Consortium, "STORK 2.0 Project," 2016, https://www.eid-stork2.eu, [Online; Accessed on June 1, 2017].

[24] STORK-eID Consortium, "D5.8.3d Security Principles and Best Practices Deliverable," 2011, https://nio.gov.si/nio/cms/download/document/2d344aa8e043711ce03d0d117b525d6f00169e7f-1342132021668, [Online; Accessed on June 1, 2017].

[25] T. Klobučar, D. Gabrijelcic, and V. Pagon, "Cross-Border e-Learning and Academic Services based on eIDs: Case of Slovenia," in *Proc. of the 2014 eChallenges e-2014 Conference, Belfast, Ireland.* IEEE, March 2014.

[26] STORK-eID Consortium, "D4.4 First version of Technical Specifications for the cross border Interface," 2011, https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=25:d44-first-version-of-technical-specifications-for-the-cross-border-interface-&Itemid=174, [Online; Ac-

cessed on June 1, 2017].

[27] European Commission, “Trust Services and eID (eIDAS regulation),” 2016, https://ec.europa.eu/digital-single-market/en/trust-services-and-eid, [Online; Accessed on June 1, 2017].

[28] eIDAS Technical Subgroup, “eIDAS - Interoperability Architecture,” 2015, https://joinup.ec.europa.eu/sites/default/files/eidas_interoperability_architecture_v1.00.pdf, [Online; Accessed on June 1, 2017].

[29] eIDAS Technical Subgroup, “eIDAS Technical Specifications v1.0,” November 2015, https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10, [Online; Accessed on June 1, 2017].

[30] T. J. Smedinghoff, “Solving the legal challenges of trustworthy online identity,” *Computer Law & Security Review*, vol. 28, no. 5, pp. 532–541, October 2012.

[31] J. Basney and S. Koranda, “A Study of Three Approaches to International Identity Federation for the LIGO Project,” 2013, https://scholarworks.iu.edu/dspace/handle/2022/16760, [Online; Accessed on June 1, 2017].

[32] D. Pöhn, S. Metzger, and W. Hommel, “Géant-TrustBroker: Dynamic, Scalable Management of SAML-Based Inter-federation Authentication and Authorization Infrastructures,” in *Proc. of the 29th International Information Security Conference (SEC’14), Marrakech, Morocco*, ser. IFIP Advances in Information and Communication Technology, vol. 428. Springer Berlin Heidelberg, June 2014.

[33] Kantara, “Kantara Project,” 2017, https://kantarainitiative.org/, [Online; Accessed on June 1, 2017].

[34] Liberty Alliance Project, “Liberty Identity Assurance Framework,” 2008, http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf, [Online; Accessed on June 1, 2017].

[35] InCommons, “InCommons Report January 2015 - June 2016,” 2016, https://www.incommon.org/docs/InCommonReport2016.pdf, [Online; Accessed on June 1, 2017].

[36] AARC, “AARC Project,” 2017, = https://aarc-project.eu/, [Online; Accessed on June 1, 2017].

[37] D. Hardt, “The OAuth 2.0 Authorization Framework [RFC 6749],” IETF RFC 6749, October 2012, https://tools.ietf.org/html/rfc6749, [Online; Accessed on June 1, 2017].

[38] E. Torroglosa-García, A. D. Pérez-Morales, P. Martinez-Julia, and D. R. Lopez, “Integration of the OAuth and Web Service family security standards,” *Computer Networks*, vol. 57, no. 10, pp. 2233–2249, July 2013.

[39] N. Sakimura, J. Bradley, M. Jones, and B. de Medeiros, “Openid connect core 1.0,” *The OpenID* {...}, November 2014.

[40] Shibboleth WIKI, “Shibboleth’s wiki webpage,” 2013, https://wiki.shibboleth.net/confluence/display/SHIB2/Home, [Online; Accessed on June 1, 2017].

[41] J. Ortiz, P. Martinez-julia, C. Kanellopoulos, and A. F. Skarmeta, “Scholar European Electronic Identity Federation,” in *Proc. of the 11th TERENA Networking Conference (TNC’15), Porto, Portugal*, June 2015, pp. 1–3.

Author Biography

Elena M. Torroglosa-Garcia is a researcher in the Department of Information and Communications Engineering of the University of Murcia since 2008, where she received her B.S. degree on Computer Science and the M.S. degree on New Technologies in Computer Science in 2012. She has been involved in multiple research projects in diverse fields such as AAA/Identity environments (SWIFT, GEMBus, STORK2.0) GN4-1-SA5-T1, GN4-2-JRA3T3), design of inter-federation solutions (GN4-1-SA5-T1: STORK2 with eduGAIN, GN4-2-JRA3T3: eIDAS with eduGAIN) and Experimentation Infrastructures such as OpenLAB. Currently, she is a PH.D. candidate at the University of Murcia and her doctoral studies are focused on analyzing and researching current security systems related to authentication, authorization and access control mechanisms typical of the current identity management systems, with the aim of achieving interoperability mechanisms between existing federations and the new technologies in the context of Future Internet to establish the necessary trust models.

Dr. Antonio F. Skarmeta-Gomez received the M.S. degree in Computer Science from the University of Granada and B.S. (Hons.) and the Ph.D. degrees in Computer Science from the University of Murcia Spain. Since 2009 he is Full Professor at the same department and University. Antonio F. Skarmeta has worked on different research projects in the national and international area in the networking, security and IoT area, like Euro6IX, ENABLE, DAIDALOS, SWIFT, SEMIRAMIS, SMARTIE, SOCIOTAL and IoT6. His main interested is in the integration of security services, identity, IoT and Smart Cities. He has been head of the research group ANTS since its creation on 1995. Actually he is also advisor to the vice-rector of Research of the University of Murcia for International projects and head of the International Research Project Office. Since 2014 he is Spanish National Representative for the MSCA within H2020. He has published over 200 international papers and being member of several program committees. He has also participated in several standardization for a like IETF, ISO and ETSI.